
Privacy
boekenwijsheid of praktijkles?
www

Jean Paul van Schoonhoven

- Directeur privacy management bureau Legal2Practice
- Public & Key note speaker
- Chief Privacy Officer PostNL
- IAPP certificeringen FIP CIPM CIPP/E CIPT
- Erkend deskundige Stimuleringskader Integere Organisatie
- Redactielid:
  - Tijdschrift voor Compliance (DenHollander)
  - Jurisprudentie Bescherming Persoonsgegevens (Sdu)
  - Rechtspraak Financieel recht (Wolters Kluwer)
- Docentschappen (ook in company) o.a.:
  - hoofddocent Privacy Officer 2.0 (IIR)
  - hoofddocent FG in de publieke sector (IIR)
  - hoofddocent PIA's in de praktijk (IIR)
  - docent Certified Data Protection Officer (IIR)
  - docent Auditing Privacy (IIR)
  - docent Privacy Awareness Gemeenten (IIR)

http://nl.linkedin.com/in/jpvanschoonhoven


Handboek Privacyrecht
cubiss

Privacy recht

Wbp 2001

AVG 2018 (80% Wbp)

Uitvoeringswet AVG 2018

Voor organisaties die al aantoonbaar voldoen aan de Wbp is de AVG een peuleschil 😊

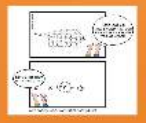
Anders liggen er behoorlijke uitdagingen in het verschiet...


'Mark my words'

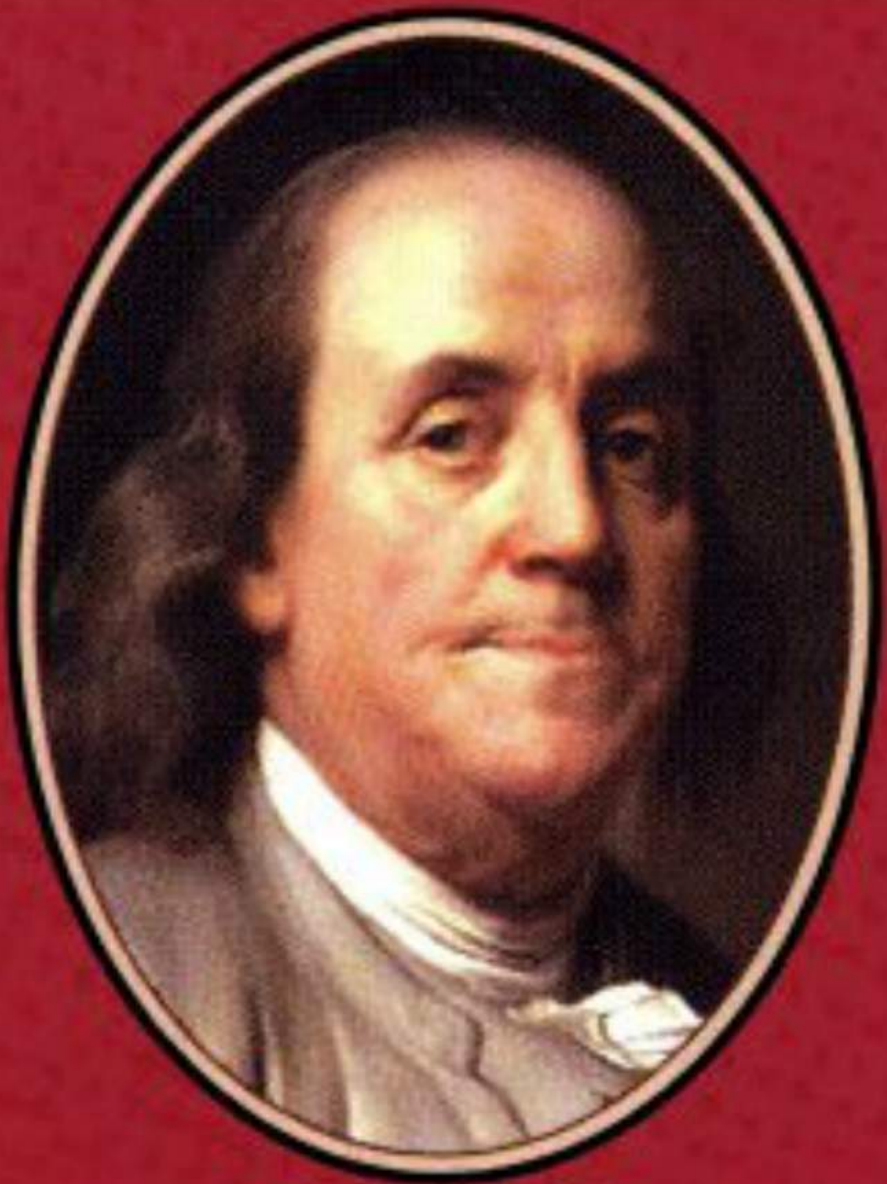
Alles is data

En bijna alle data zijn persoonsgegevens
Maar we zitten met een privacy paradox



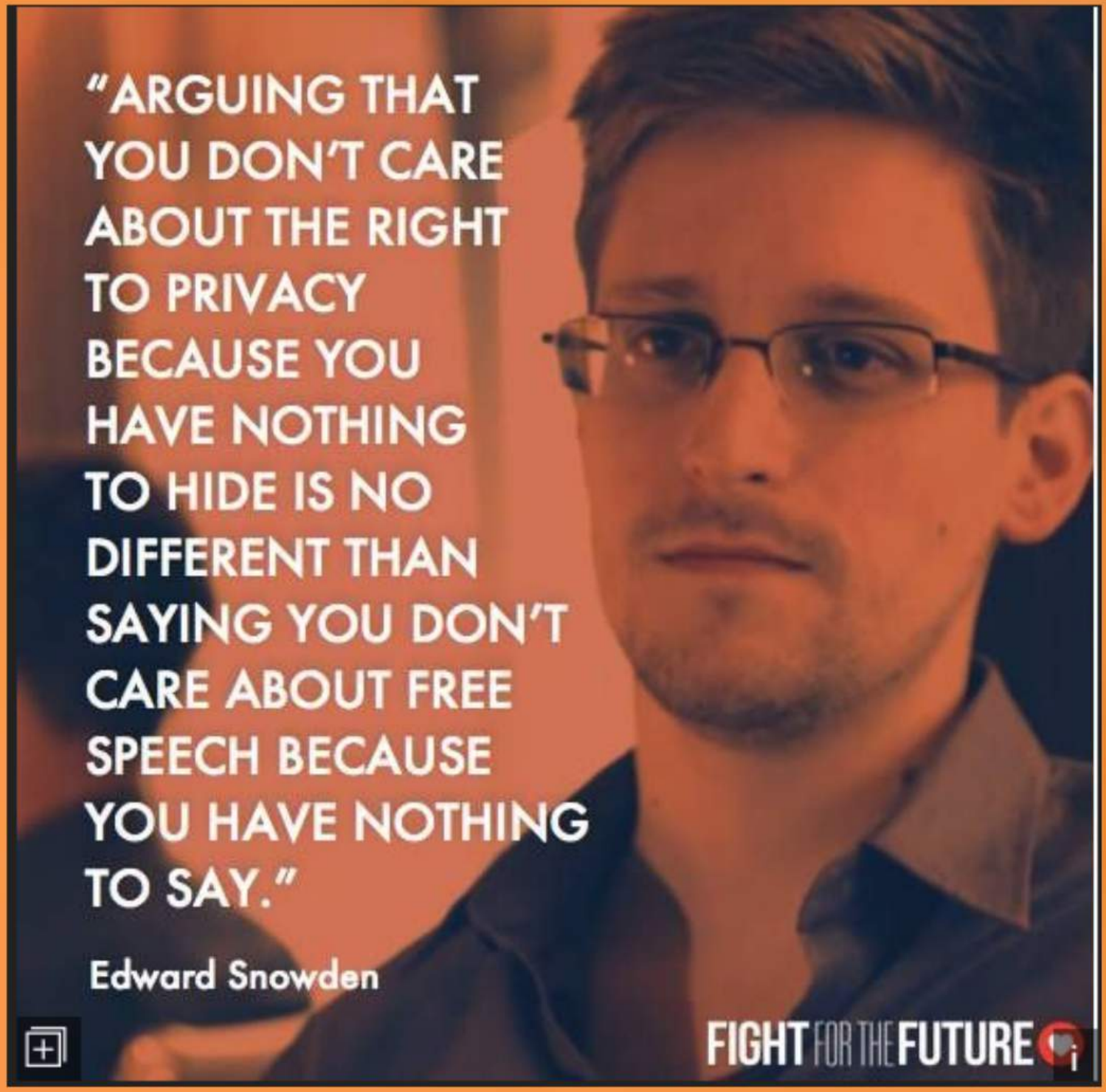





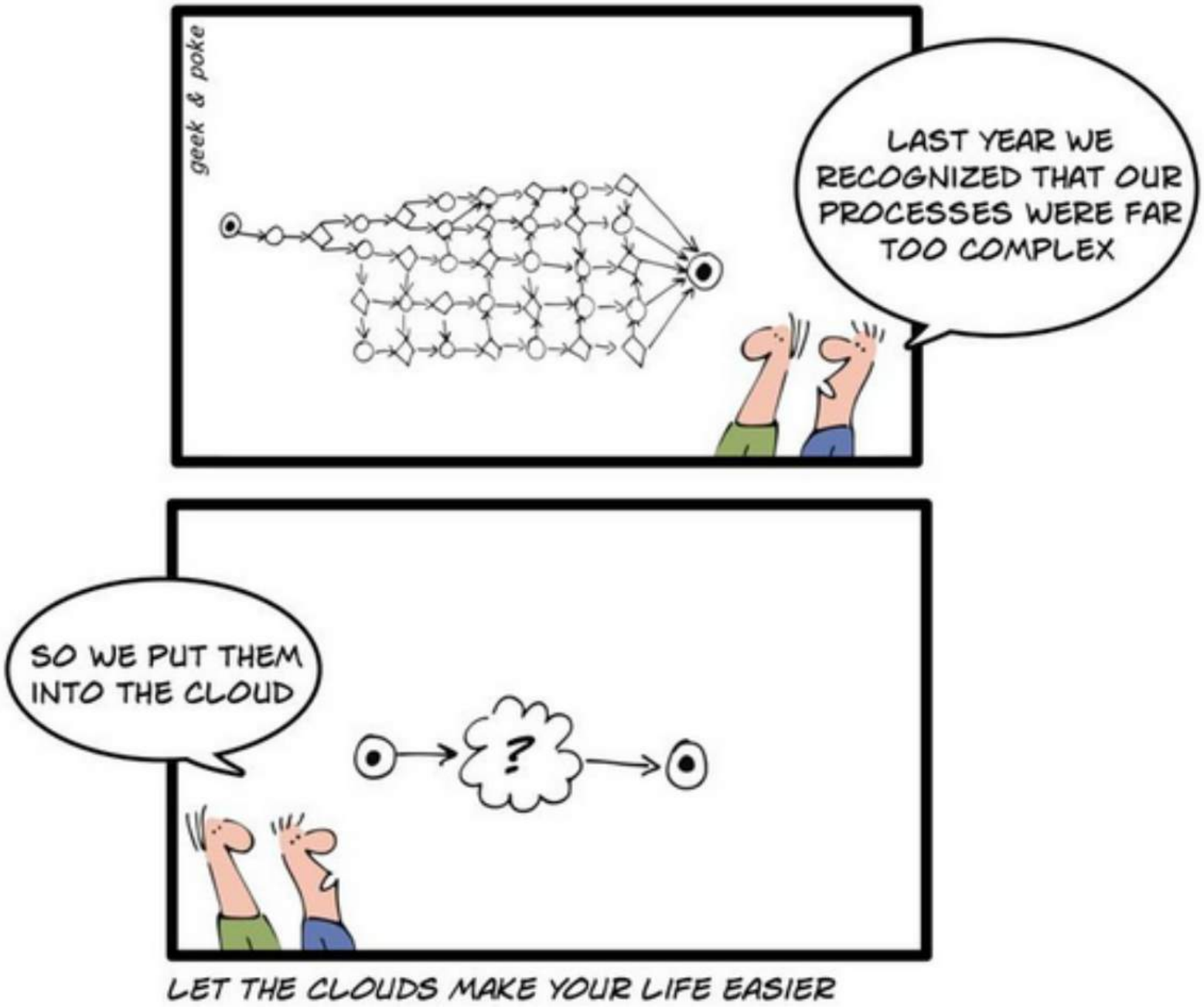


"Any society that would give up a little liberty to gain a little security will deserve neither and lose both."

-Benjamin Franklin


"ARGUING THAT YOU DON'T CARE ABOUT THE RIGHT TO PRIVACY BECAUSE YOU HAVE NOTHING TO HIDE IS NO DIFFERENT THAN SAYING YOU DON'T CARE ABOUT FREE SPEECH BECAUSE YOU HAVE NOTHING TO SAY."
Edward Snowden
FIGHT FOR THE FUTURE


GET ALL THE INFORMATION YOU CAN, WE'LL THINK OF A USE FOR IT LATER.
SLANE


geek & poke
LAST YEAR WE RECOGNIZED THAT OUR PROCESSES WERE FAR TOO COMPLEX
SO WE PUT THEM INTO THE CLOUD
?
LET THE CLOUDS MAKE YOUR LIFE EASIER

REGISTREER INLOGGEN

TWITTER TIP DE REDACTIE APP'S

spitsnieuws.nl

SPITS

Nieuws & Entertainment

WORD OOK EEN HER

ALLES BINNENLAND ENTERTAINMENT

Werknemer laks met data

Een derde van de werknemers slaat zakelijke informatie op in de cloud, zonder zich daarbij voldoende af te vragen of dit wel veilig is. Het grootste gedeelte van de werknemers maakt inmiddels gebruik van meerdere apparaten om zijn of haar werk te kunnen doen. Daarom wordt er steeds vaker gebruik gemaakt van online diensten om bestanden te delen. Volgens onderzoek van IT-bedrijf Fujitsu staan bedrijven en werknemers er onvoldoende bij stil dat zij daarmee mogelijk grote risico´s lopen.

MOActivities

- MOA Digital Analytics Middag
- BkB bijeenkomsten
- MOA Circles
- MOA/NIMA Education Days (sectie onderwijs)
- Symposium Tickle Your Senses (Sensorisch onderzoek)
- Healthcare Symposia
- SMART bijeenkomsten
- Greyhounds bijeenkomsten

Agenda

Privacybeleving op het internet in Nederland

apr 29, 2015 | lettergrootte | Print | E-mailadres

Gepubliceerd in
Actueel

Lees
2180 keer

Beoordeel dit item
★ ★ ★ ★ ★
(0 stemmen)

Getagged onder
Privacybeleving
Internet
Consumentenonderzoek
ClouToday79

Op het gebied van privacy is afgelopen maand een belangrijk rapport van TNO gepubliceerd: 'Privacybeleving op het internet in Nederland'.

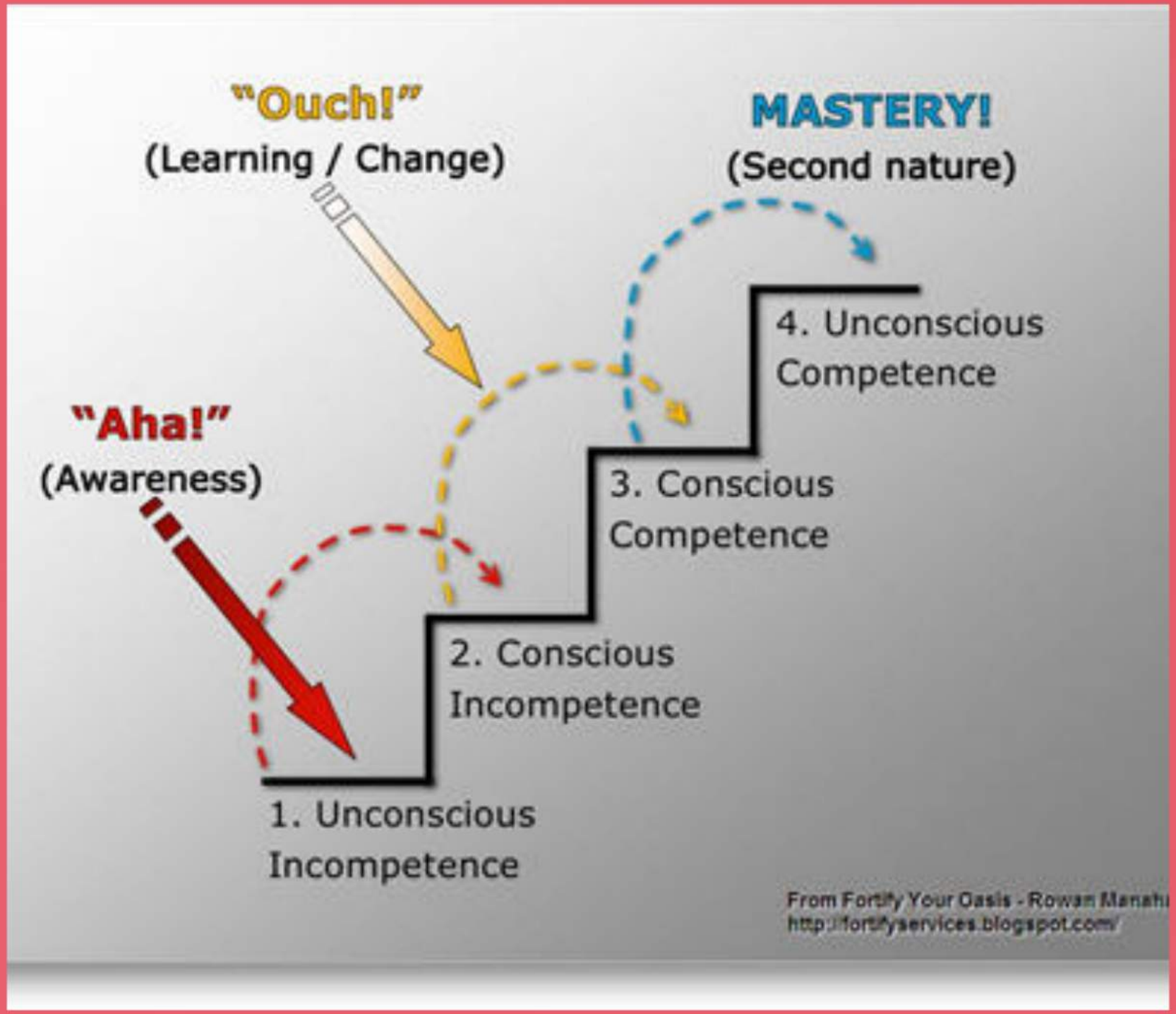
De MOA zette de belangrijkste conclusies op een rij:

- Om inzicht te geven in de privacybeleving van de Nederlands samenleving is een onderzoek uitgevoerd naar ruim 1000 Nederlandse consumenten.
- Uit het onderzoek blijkt dat de Nederlandse bevolking relatief veel belang hecht aan privacy en bescherming van persoonsgegevens.
- Er is veel onduidelijkheid over hoe mensen meer controle kunnen uitoefenen over hun persoonsgegevens en het gebruik daarvan door anderen, met name door commerciële partijen.
- Leeftijd hangt samen met de bereidheid om gegevens te delen. Jong volwassenen (18-34) blijken de bescherming van persoonsgegevens minder belangrijk te vinden. Dit komt o.a. doordat zij het delen van informatie een vanzelfsprekendheid vinden in de huidige maatschappij.
- Ook blijkt uit het onderzoek dat het gebruik maken van diensten vaak doorslaggevend is in de afweging of iemand wel of geen persoonsgegevens deelt. Er is sprake van een privacy paradox. Het belang van privacy wordt door het overgrote deel van de mensen benadrukt, maar toch worden gegevens vaak verstrekt als daarom wordt gevraagd.
- Bijna de helft (!) van de Nederlanders leest de algemene voorwaarden, net als in Canada en Australië. Dit terwijl algemene voorwaarden vaak onduidelijk en lang worden gevonden.
- **Overheidsorganisaties, zoals de politiek en de belastingdienst, maar ook de gezondheidszorg, werkgevers, verzekeraars en banken worden meer vertrouwd in het gebruik en de bescherming van persoonsgegevens dan commerciële organisaties, zoals webwinkels, goede doelenorganisaties en marktonderzoeksbureaus.**
- Het valt op dat de vormen van privacy waaraan veel belang wordt gehecht, samenhangen met online privacy en privacy van informatie. Er lijkt een verband te bestaan tussen de mate van beslotenheid en de privacy verwachting die daarbij hoort.
- De privacy paradox: hoewel mensen belang hechten aan privacy en de bescherming van persoonsgegevens en ook beschermende software installeren, is met toch bereid om gegevens te delen als dit voor het gebruik van een dienst noodzakelijk is. Dit is onder andere het gevolg van 'peer pressure'. Meer dan 40% geeft aan weleens het gevoel te hebben dat ze wel aan een dienst moeten deelnemen, omdat iedereen in hun omgeving dat doet.

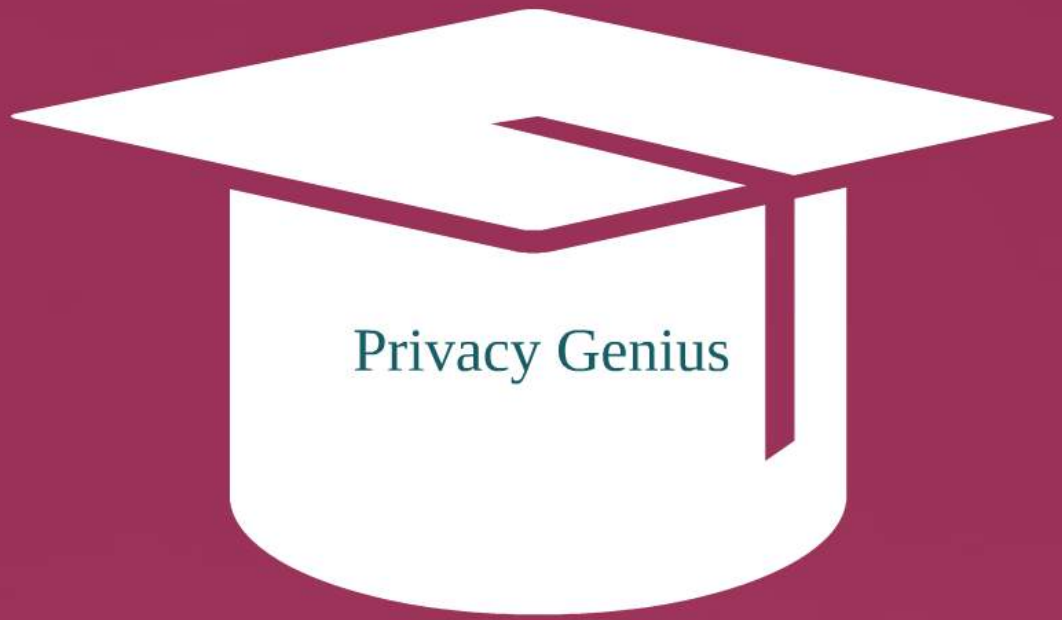

S?
Ok, ik heb jullie aandacht

Ok, ik heb jullie aandacht

Maar bedenk dit:


"Ouch!"
(Learning / Change)
MASTERY!
(Second nature)
4. Unconscious Competence
"Aha!"
(Awareness)
3. Conscious Competence
2. Conscious Incompetence
1. Unconscious Incompetence
From Fortify Your Oasis - Rowan Manahi
http://fortifyservices.blogspot.com/


KEN JE DE FUNDAMENTELE ATTRIBUTIEFOUT? HUN **EIGEN** FALEN SCHRIJVEN MENSEN TOE AAN INCOMPETENTIE.
MAAR FOUTEN VAN **ANDEREN** WORDEN DAARENTEGEN TOE-GESCHREVEN AAN EXTERNE OMSTANDIGHEDEN.
VOLGENS MIJ IS HET ANDERSOM.
NEE, JIJ BENT TE DOM OM MIJN UITLEG TE BEGRIJPEN!
15-8/569

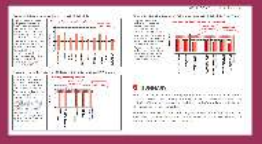

Privacy Genius

In 10 stappen naar het privacy walhalla



Dat is overzichtelijker dan dit:

Of dit:

pen naar het

AUTORITEIT PERSOONSGEGEVENS

In 10 stappen voorbereid op de AVG

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Wat verandert er?

De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt – meer dan nu – op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden.

Wat kan ik doen?

Als organisatie kunt u nu alvast stappen ondernemen om straks klaar te zijn voor de AVG. Om u hierbij te helpen, heeft de Autoriteit Persoonsgegevens de 10 belangrijkste stappen voor u op een rijtje gezet.

Stap 1: Bewustwording

Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

De Autoriteit Persoonsgegevens (AP) biedt instrumenten die u kunnen helpen om de AVG na te leven, zoals guidelines die zijn opgesteld samen met de andere privacytoezichthouders in Europa.

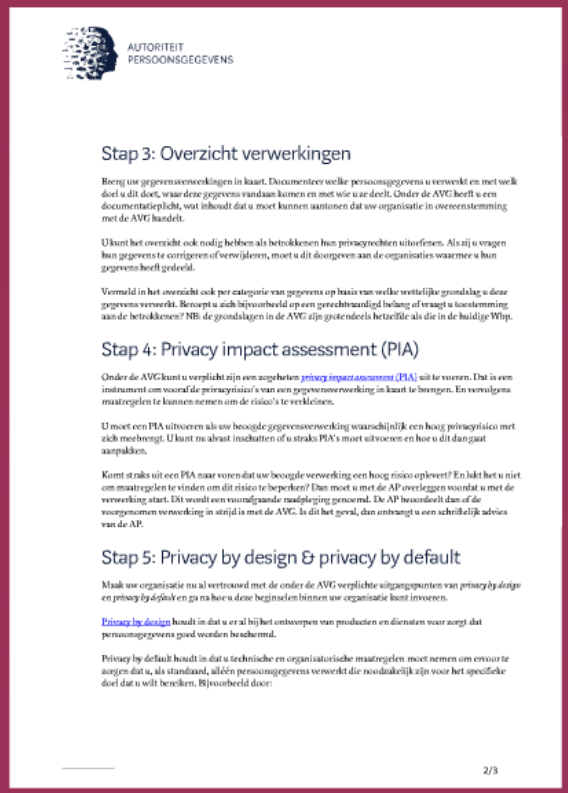
Bedenk dat de AP uw organisatie sancties kan opleggen van maximaal 20 miljoen euro of 4% van uw wereldwijde omzet als u zich niet aan de nieuwe privacywetgeving houdt.

Stap 2: Rechten van betrokkenen

Onder de AVG krijgen betrokkenen (de mensen van wie u persoonsgegevens verwerkt) meer en verbeterde privacyrechten. Zorg er daarom voor dat zij hun privacyrechten goed kunnen uitoefenen. Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering.

Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Ook kunnen mensen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.



AUTORITEIT PERSOONSGEGEVENS

Stap 3: Overzicht verwerkingen

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt. Onder de AVG heeft u een documentatieplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt.

U kunt het overzicht ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

Vermeld in het overzicht ook per categorie van gegevens op basis van welke wettelijke grondslag u deze gegevens verwerkt. Beroept u zich bijvoorbeeld op een gerechtvaardigd belang of vraagt u toestemming aan de betrokkenen? NB: de grondslagen in de AVG zijn grotendeels hetzelfde als die in de huidige Wbp.

Stap 4: Privacy impact assessment (PIA)

Onder de AVG kunt u verplicht zijn een zogeheten privacy impact assessment (PIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

U moet een PIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks PIA's moet uitvoeren en hoe u dit dan gaat aanpakken.

Komt straks uit een PIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te vinden om dit risico te beperken? Dan moet u met de AP overleggen voordat u met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangt u een schriftelijk advies van de AP.

Stap 5: Privacy by design & privacy by default

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van *privacy by design* en *privacy by default* en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

AUTORITEIT PERSOONSGEGEVENS

- een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken;
- als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

Stap 6: Functionaris voor de gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie geldt. Zo ja, wacht dan niet te lang met het werven van een FG. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

Stap 7: Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken.

Stap 8: Bewerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een bewerker (in de AVG 'verwerker' genoemd)? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Stap 9: Leidende toezichthouder

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Dit wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.

Stap 10: Toestemming

Uw gegevensverwerking kan gebaseerd zijn op toestemming van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan. Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

is overzichtelijker dan di

AUTORITEIT
PERSOONSGEGEVENS

In 10 stappen voorbereid op de AVG

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Wat verandert er?

De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt – meer dan nu – op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zich aan de wet houden.

Wat kan ik doen?

Als organisatie kunt u nu alvast stappen ondernemen om straks klaar te zijn voor de AVG. Om u hierbij te helpen, heeft de Autoriteit Persoonsgegevens de 10 belangrijkste stappen voor u op een rijtje gezet.

Stap 1: Bewustwording

Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

De Autoriteit Persoonsgegevens (AP) biedt instrumenten die u kunnen helpen om de AVG na te leven, zoals guidelines die zijn opgesteld samen met de andere privacytoezichthouders in Europa.

Bedenk dat de AP uw organisatie sancties kan opleggen van maximaal 20 miljoen euro of 4% van uw wereldwijde omzet als u zich niet aan de nieuwe privacywetgeving houdt.

Stap 2: Rechten van betrokkenen

Onder de AVG krijgen betrokkenen (de mensen van wie u persoonsgegevens verwerkt) meer en verbeterde privacyrechten. Zorg er daarom voor dat zij hun privacyrechten goed kunnen uitoefenen. Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering.

Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Ook kunnen mensen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

Stap 3: Overzicht verwerkingen

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt. Onder de AVG heeft u een documentatieplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt.

U kunt het overzicht ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

Vermeld in het overzicht ook per categorie van gegevens op basis van welke wettelijke grondslag u deze gegevens verwerkt. Beroept u zich bijvoorbeeld op een gerechtvaardigd belang of vraagt u toestemming aan de betrokkenen? NB: de grondslagen in de AVG zijn grotendeels hetzelfde als die in de huidige Wbp.

Stap 4: Privacy impact assessment (PIA)

Onder de AVG kunt u verplicht zijn een zogeheten *privacy impact assessment* (PIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

U moet een PIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks PIA's moet uitvoeren en hoe u dit dan gaat aanpakken.

Komt straks uit een PIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te vinden om dit risico te beperken? Dan moet u met de AP overleggen voordat u met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangt u een schriftelijk advies van de AP.

Stap 5: Privacy by design & privacy by default

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van *privacy by design* en *privacy by default* en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

- een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken;
- als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

Stap 6: Functionaris voor de gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie geldt. Zo ja, wacht dan niet te lang met het werven van een FG. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

Stap 7: Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken.

Stap 8: Bewerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een bewerker (in de AVG 'verwerker' genoemd)? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Stap 9: Leidende toezichthouder

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Dit wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.

Stap 10: Toestemming

Uw gegevensverwerking kan gebaseerd zijn op toestemming van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan. Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

UPDATED JANUARY 2017

Nymity Privacy Management Accountability Framework™

A menu of privacy management activities (technical and organisational measures)

NYMITY
innovating compliance

1. Maintain Governance Structure

Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures

Privacy Management Activities

- Assign responsibility for data privacy to an individual (e.g. Privacy Officer, Privacy Counsel, CPO, Representative)
- Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)
- Appoint a Data Protection Officer/Official (DPO) in an independent oversight role
- Assign responsibility for data privacy throughout the organization (e.g. Privacy Network)
- Maintain roles and responsibilities for individuals responsible for data privacy (e.g. job descriptions)
- Conduct regular communication between the privacy office, privacy network and others responsible/accountable for data privacy
- Engage stakeholders throughout the organization on data privacy matters (e.g. information security, marketing, etc.)
- Report to internal stakeholders on the status of privacy management (e.g. board of directors, management)
- Report to external stakeholders on the status of privacy management (e.g. regulators, third-parties, clients)
- Conduct an Enterprise Privacy Risk Assessment
- Integrate data privacy into business risk assessments/reporting
- Maintain a Privacy Strategy
- Maintain a privacy program charter/mission statement
- Require employees to acknowledge and agree to adhere to the data privacy policies

2. Maintain Personal Data Inventory and Data Transfer Mechanisms

Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border, with defined classes of personal data

Privacy Management Activities

- Maintain an inventory of personal data holdings (what personal data is held and where)
- Classify personal data holdings by type (e.g. sensitive, confidential, public)
- Obtain regulator approval for data processing (where prior approval is required)
- Register databases with regulators (where registration is required)
- Maintain flow charts for data flows (e.g. between systems, between processes, between countries)
- Maintain records of the transfer mechanism used for cross-border data flows (e.g. standard contractual clauses, binding corporate rules, approvals from regulators)
- Use Binding Corporate Rules as a data transfer mechanism
- Use contracts as a data transfer mechanism (e.g. Standard Contractual Clauses)
- Use APEC Cross Border Privacy Rules as a data transfer mechanism
- Use the EU-US Privacy Shield as a data transfer mechanism
- Use regulator approval as a data transfer mechanism
- Use adequacy or one of the derogations from adequacy (e.g. consent, performance of a contract, public interest) as a data transfer mechanism

3. Maintain Internal Data Privacy Policy

Maintain a data privacy policy that meets legal requirements and addresses operational risk and risk of harm to individuals

Privacy Management Activities

- Maintain a data privacy policy
- Maintain an employee data privacy policy
- Maintain an organizational code of conduct that includes privacy
- Document legal basis for processing personal data
- Integrate ethics into data processing (Codes of Conduct, policies and other measures)

4. Embed Data Privacy Into Operations

Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

Privacy Management Activities

- Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)
- Maintain policies/procedures for collection and use of children and minors' personal data
- Maintain policies/procedures for maintaining data quality
- Maintain policies/procedures for the de-identification of personal data
- Maintain policies/procedures to review processing conducted wholly or partially by automated means
- Maintain policies/procedures for secondary uses of personal data
- Maintain policies/procedures for obtaining valid consent
- Maintain policies/procedures for secure destruction of personal data
- Integrate data privacy into use of cookies and tracking mechanisms
- Integrate data privacy into records retention practices
- Integrate data privacy into direct marketing practices
- Integrate data privacy into e-mail marketing practices
- Integrate data privacy into telemarketing practices
- Integrate data privacy into digital advertising practices (e.g. online, mobile)
- Integrate data privacy into hiring practices
- Integrate data privacy into the organization's use of social media
- Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures
- Integrate data privacy into health & safety practices
- Integrate data privacy into interactions with works councils
- Integrate data privacy into practices for monitoring employees
- Integrate data privacy into use of CCTV/video surveillance
- Integrate data privacy into use of geo-location (tracking and or location) devices
- Integrate data privacy into policies/procedures regarding access to employees' company e-mail accounts
- Integrate data privacy into e-discovery practices
- Integrate data privacy into conducting internal investigations
- Integrate data privacy into practices for disclosure to and for law enforcement purposes
- Integrate data privacy into research practices (e.g. scientific and historical research)

5. Maintain Training and Awareness Program

Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks

Privacy Management Activities

- Conduct privacy training
- Conduct privacy training reflecting job specific content
- Conduct regular refresher training
- Incorporate data privacy into operational training, such as HR, security, call centre
- Deliver training/awareness in response to timely issues/topics
- Deliver a privacy newsletter, or incorporate privacy into existing corporate communications
- Provide a repository of privacy information (e.g. an internal data privacy intranet)
- Maintain privacy awareness material (e.g. posters and videos)
- Conduct privacy awareness events (e.g. an annual data privacy day/week)
- Measure participation in data privacy training activities (e.g. number of participants, scoring)
- Enforce the requirement to complete privacy training
- Provide ongoing education and training for the Privacy Office and/or DPOs
- Maintain certification for individuals responsible for data privacy, including continuing professional education

6. Manage Information Security Risk

Maintain an information security program based on legal requirements and ongoing risk assessments

Privacy Management Activities

- Integrate data privacy risk into security risk assessments
- Integrate data privacy into an information security policy
- Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
- Maintain measures to encrypt personal data
- Maintain an acceptable use of information resources policy
- Maintain procedures to restrict access to personal data (e.g. role-based access, segregation of duties)
- Integrate data privacy into a corporate security policy (protection of physical premises and hard assets)
- Maintain human resource security measures (e.g. pre-screening, performance appraisals)
- Integrate data privacy into business continuity plans
- Maintain a data-loss prevention strategy
- Conduct regular testing of data security posture
- Maintain a security certification (e.g. ISO)

7. Manage Third-Party Risk

Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance

Privacy Management Activities

- Maintain data privacy requirements for third parties (e.g. clients, vendors, processors, affiliates)
- Maintain procedures to execute contracts or agreements with all processors
- Conduct due diligence around the data privacy and security posture of potential vendors/processors
- Conduct due diligence on third party data sources
- Maintain a vendor data privacy risk assessment process
- Maintain a policy governing use of cloud providers
- Maintain procedures to address instances of non-compliance with contracts and agreements
- Conduct ongoing due diligence around the data privacy and security posture of vendors/processors
- Review long-term contracts for new or evolving data privacy risks

8. Maintain Notices

Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance

Privacy Management Activities

- Maintain a data privacy notice that details the organization's personal data handling practices
- Provide data privacy notice at all points where personal data is collected
- Provide notice by means of on-location signage, posters
- Provide notice in marketing communications (e.g. emails, flyers, offers)
- Provide notice in contracts and terms
- Maintain scripts for use by employees to explain or provide the data privacy notice
- Maintain a privacy Seal or Trustmark on the website to increase customer trust

9. Respond to Requests and Complaints from Individuals

Maintain effective procedures for interactions with individuals about their personal data

Privacy Management Activities

- Maintain procedures to address complaints
- Maintain procedures to respond to requests for access to personal data
- Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data
- Maintain procedures to respond to requests to opt-out of, restrict or object to processing
- Maintain procedures to respond to requests for information
- Maintain procedures to respond to requests for data portability
- Maintain procedures to respond to requests to be forgotten or for erasure of data
- Maintain Frequently Asked Questions to respond to queries from individuals
- Investigate root causes of data privacy complaints
- Monitor and report metrics for data privacy complaints (e.g. number, root cause)

10. Monitor for New Operational Practices

Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles

Privacy Management Activities

- Integrate Privacy by Design into system and product development
- Maintain PIA/DPIA guidelines and templates
- Conduct PIAs/DPIAs for new programs, systems, processes
- Conduct PIAs or DPIAs for changes to existing programs, systems, or processes
- Engage external stakeholders (e.g., individuals, privacy advocates) as part of the PIA/DPIA process
- Track and address data protection issues identified during PIAs/DPIAs
- Report PIA/DPIA analysis and results to regulators (where required) and external stakeholders (if appropriate)

11. Maintain Data Privacy Breach Management Program

Maintain an effective data privacy incident and breach management program

Privacy Management Activities

- Maintain a data privacy incident/breach response plan
- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol
- Maintain a log to track data privacy incidents/breaches
- Monitor and report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)
- Conduct periodic testing of data privacy incident/breach plan
- Engage a breach response remediation provider
- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage

12. Monitor Data Handling Practices

Verify operational practices comply with the data privacy policy and operational policies and procedures, and measure and report on their effectiveness

Privacy Management Activities

- Conduct self-assessments of privacy management
- Conduct Internal Audits of the privacy program (i.e. operational audit of the Privacy Office)
- Conduct ad-hoc walk-throughs
- Conduct ad-hoc assessments based on external events, such as complaints/breaches
- Engage a third party to conduct audits/assessments
- Monitor and report privacy management metrics
- Maintain documentation as evidence to demonstrate compliance and/or accountability
- Maintain certifications, accreditations or data protection seals for demonstrating compliance to regulators

13. Track External Criteria

Track new compliance requirements, expectations, and best practices

Privacy Management Activities

- Identify ongoing privacy compliance requirements e.g., law, case law, codes, etc.
- Maintain subscriptions to compliance reporting service/law firm updates to stay informed of new developments
- Attend/participate in privacy conferences, industry association, or think-tank events
- Record/report on the tracking of new laws, regulations, amendments or other rule sources
- Seek legal opinions regarding recent developments in law
- Identify and manage conflicts in law
- Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes

The Nymity Privacy Management Accountability Framework™ was developed based on Nymity's global research on data privacy accountability.
The Framework is a comprehensive listing of over 130 Privacy Management Activities (PMAs) categorized into 13 Privacy Management Categories (PMCs).

Of dit:

Figure 1 – Privacy Maturity Report by GAPP Principle

Figure 1 shows a sample graph that could be used to illustrate the maturity of the organization's privacy program by each of the 10 principles in GAPP.

The report also indicates the desired maturity level for the enterprise.

Reports like this are useful in providing management with an overview of the entity's privacy program and initiatives.

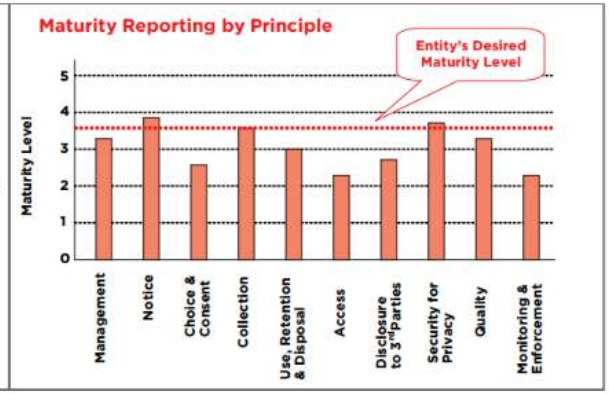


Figure 2 – Maturity Report by Criteria within a Specific GAPP Principle

Figure 2 shows the maturity of each criterion within a specific principle – in this case, the 'Notice' principle.

The report indicates the actual maturity level for each criterion.

The report also indicates the actual and desired maturity level for the principle as a whole.

Reports like this provide useful insight into specific criteria within a privacy principle.

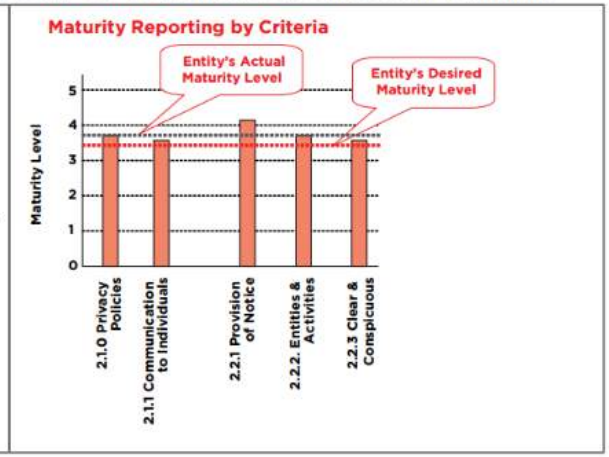
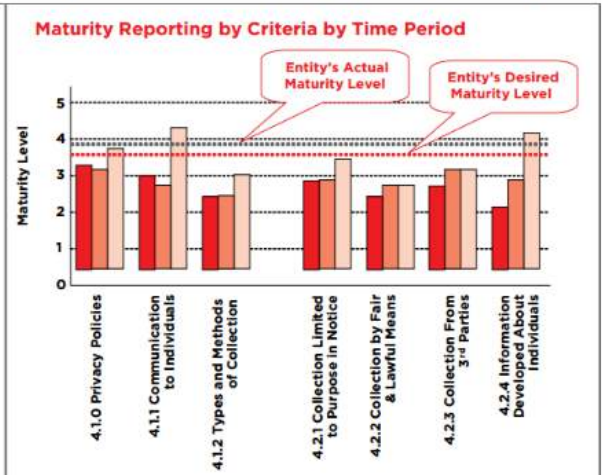


Figure 3 – Maturity Report by Criteria within a GAPP Principle Over Time

Figure 3 shows the maturity of each criterion within the 'Collection' principle for three time periods.

The report indicates the actual maturity level for each criterion for three different time periods.

Reports like this provide useful insight into progress being made by the entity's privacy initiatives over time.



6 SUMMARY

The AICPA/CICA Privacy Maturity Model provides entities with an opportunity to assess their privacy initiatives against criteria that reflect the maturity of their privacy program and their level of compliance with Generally Accepted Privacy Principles.

The PMM can be a useful tool for management, consultants and auditors and should be considered throughout the entity's journey to develop a strong privacy program and benchmark its progress.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
SECURITY FOR PRIVACY (9 criteria) cont.	**The entity protects personal information against unauthorized access (both physical and logical).**					
Logical Access Controls (8.2.2)	**Logical access to personal information is restricted by procedures that address the following matters:** **a. Authorizing and registering internal personnel and individuals** **b. Identifying and authenticating internal personnel and individuals** **c. Making changes and updating access profiles** **d. Granting privileges and permissions for access to IT infrastructure components and personal information** **e. Preventing individuals from accessing anything other than their own personal or sensitive information** **f. Limiting access to personal information only to authorized internal personnel based upon their assigned roles and responsibilities** **g. Distributing output only to authorized internal personnel** **h. Restricting logical access to offline storage, backup data, systems and media** **i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)** **j. Preventing the introduction of viruses, malicious code, and unauthorized software**	Controls over access and privileges to files and databases containing personal information are informal, inconsistent and incomplete.	The entity has basic security procedures; however, they do not include specific requirements governing logical access to personal information and may not provide an appropriate level of access or control over personal information.	The entity has documented and implemented security policies and procedures that sufficiently control access to personal information. Access to personal information is restricted to employees with a need for such access.	Management monitors logical access controls, including access attempts and violation reports for files, databases and resources containing personal information to identify areas where additional security needs improvement. Irregular access of authorized personnel is also monitored.	Access and violation attempts are assessed to determine root causes and potential exposures and remedial action plans are developed and implemented to increase the level of protection of personal information. Logical access controls are continually assessed and improved. Irregular access of authorized personnel is monitored, assessed and investigated where necessary.


www

Beveilig de data passend

Anonimiseer, pseudonimiseer en encrypt

- Het gaat dus mis voordat je het weet
- Meeste datalekken zijn interne fouten
- Boete schending meldplicht tot €500k

AUTORITEIT
PERSOONSGEGEVENS

TIP ONS

Home Actueel Over privacy Onderwerpen Zelf doen Publicaties Melden

AP adviseert over pseudonimisering in het onderwijs

Nieuwsbericht / 23 november 2016

Categorie:
Gebruik van persoonsgegevens in het onderwijs

De Autoriteit Persoonsgegevens (AP) heeft geadviseerd over het pseudonimiseren van gegevens van leerlingen. Het wetsvoorstel houdt in dat het persoonsgebonden nummer (PGN) van een leerling gebruikt kan worden om een pseudoniem te maken. Met dit pseudoniem krijgt de leerling vervolgens toegang tot digitale leermiddelen en digitale toetsen. Daarnaast geeft het wetsvoorstel een grondslag om voor andere doelen andere pseudoniemen te genereren. De AP adviseert om het wetsvoorstel

Publicaties

Wetgevingsadvies / 8 november 2016

PDF Advies pseudonimisering onderwijs

DOWNLOADEN

AUTORITEIT
PERSOONSGEGEVENS

1 jaar meldplicht datalekken: facts & figures 2016

In de periode 1 januari tot en met 15 december 2016 zijn bijna 5500 datalekken gemeld aan de Autoriteit Persoonsgegevens (AP). Een overzicht van feiten en cijfers.

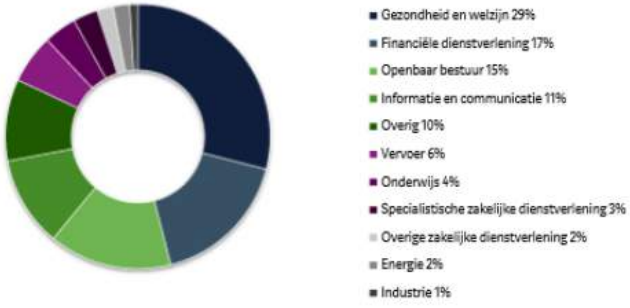
Regelmatig voorkomende datalekken

- Een klant ziet in een klantportaal de gegevens van iemand anders.
- Iemand raakt een USB-stick of andere gegevensdrager kwijt waarop persoonsgegevens staan. De persoonsgegevens zijn dan vaak niet versleuteld.
- Een laptop of smartphone waar persoonsgegevens op staan wordt gestolen.
- Een poststuk met persoonsgegevens komt niet aan bij de ontvanger of komt geopend terug.
- Een e-mail met persoonsgegevens komt bij de verkeerde ontvanger terecht.

Hoeveel mensen worden geraakt door de datalekken die zijn gemeld?

Het aantal mensen dat wordt geraakt door een datalek varieert per melding van één enkel persoon tot en met -in enkele gevallen- honderdduizenden betrokkenen.

Meldingen per sector



Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

AUTORITEIT
PERSOONSGEGEVENS

Wat valt op?

In de sectoren 'gezondheid en welzijn', 'financiële dienstverlening' en 'openbaar bestuur' worden veel persoonsgegevens verwerkt. Vaak gaat het daarbij om gevoelige persoonsgegevens zoals gezondheidsgegevens, financiële gegevens en/of het burgerservicenummer (BSN). Een datalek in één van deze sectoren zal daarom in veel gevallen leiden tot een melding aan de AP.

Binnen 'gezondheid en welzijn' waren onder meer meldingen van zorgverzekeraars, ziekenhuizen en bedrijven die bijvoorbeeld medische onderzoeken uitvoeren. Bij 'financiële dienstverlening' gaat het bijvoorbeeld om banken, verzekeraars en pensioenfondsen.

Tips over onvoldoende beveiliging

De AP heeft de indruk dat de bewustwording over het belang van beveiliging van persoonsgegevens bij mensen is gegroeid. Regelmatig ontvangt de AP tips en signalen over mogelijk onvoldoende beveiliging bij organisaties. Naar aanleiding hiervan heeft de AP meer dan 100 organisaties waarschuwingen gegeven dat zij hun beveiliging op orde moeten brengen omdat er mogelijk een datalek kan ontstaan.

Welke actie heeft de Autoriteit Persoonsgegevens tot nu toe ondernomen?

Actie vanuit de Autoriteit Persoonsgegevens kan onder meer inhouden dat

- de AP naar aanleiding van een melding contact opneemt met een organisatie om de informatie in een melding te verifiëren en zo nodig aan te vullen.
- de AP een eerste of nader onderzoek instelt of overgaat tot handhaving.
- de AP verantwoordelijken wijst op de plicht om betrokkenen, de mensen van wie de gegevens zijn gelekt, op de hoogte te stellen.
- de AP besluit tot (algemene) voorlichting naar aanleiding van een binnengekomen melding. Dit doet zij onder meer om andere organisaties bewust te maken van mogelijke beveiligingsrisico's.

Van de ongeveer 5500 meldingen heeft de AP in ruim 4000 gevallen een eerste oriënterende onderzoek gedaan. Ruim 100 organisaties kregen naar aanleiding hiervan een waarschuwing van de AP. In enkele andere tientallen gevallen is er sprake van een diepgaander onderzoek van de AP.

Over de meldingen bij de Autoriteit Persoonsgegevens

Het is belangrijk dat organisaties gegevens over de beveiliging van persoonsgegevens of over gelekte persoonsgegevens vertrouwelijk kunnen melden. De AP doet daarom geen uitspraken over specifieke meldingen. Wel geeft de AP algemene, anonieme informatie over de meldingen in jaarverslagen of andere publicaties.

- Het gaat dus mis voordat je het weet
- Meeste datalekken zijn interne fouten
- Boete schending meldplicht tot €500k

boe

INTERVIEW JACOB KOHNSTAMM

'Privacy wordt zeker chefsache, met boetes van 2% tot 4% van de omzet'

Bewaker van persoonsgegevens vertrekt na twaalf jaar bij toezichthouder

CV

1949
Geboren in Wassenaar

Studie rechten aan de Universiteit van Amsterdam (afgerond in 1977), daarna afwisselend advocaat, lid van de Tweede Kamer voor D66 en voorzitter van de partij

1994-1998
Staatssecretaris van Binnenlandse Zaken, verantwoordelijk voor grotestedenbeleid

1999-2004
Senator voor D66

2004-zomer 2016
Voorzitter van het College bescherming persoonsgegevens (CBP), dat sinds dit jaar Autoriteit Persoonsgegevens heet

2010-2014
Voorzitter van de Artikel 29-werkgroep, de Europese privacytoezichthouders

Sinds april
Coördinerend voorzitter van de Regionale Toetsingscommissies

CHEFSACHE

Bestuurders aansprakelijk na ernstige cyberaanval

Al jaren lezen wij in de krant dat cybersecurity een groeiend maatschappelijk probleem is. Maar of de toenemende zorgen organisaties daadwerkelijk aanzetten tot actie bleef lang de vraag. Het antwoord wordt steeds duidelijker. Handhavingsboetes bij ernstige datalekken kunnen onder de nieuwe Europese datawetgeving oplopen tot 4% van de wereldwijde jaaromzet. Bovendien kunnen bestuurders persoonlijk aansprakelijk gesteld worden bij ernstige cyberaanvallen, en zijn de eerste schadeclaims al een feit. Cyberaanvallen kunnen zowel ondernemingen als individuele bestuurders diep in de portemonnee raken. Cybersecurity is chefsache.

Gregg Steinhafel stapte in mei 2015 op als ceo van de Amerikaanse retailer Target, na een creditcard-hack vlak voor kerst. Target moest de klanten een persoonlijke e-mail sturen en liep miljoenen mis omdat zij hun kerstinkopen vervolgens bij de concurrent deden. Later bleek de hack niet een kleine subgroep maar 70 miljoen klanten te hebben getroffen. Target had dit verzwegen. De koers kelderde, exit Steinhafel.

Door een zware hack in 2011 bij de kleine Beverwijkse certificatenaanbieder Diginotar lag het Nederlandse internet een week plat, vooral in de publieke sector. Daarop ging Diginotar vrij snel failliet. Kort voor de hack was Diginotar overgenomen. De nieuwe eigenaar wist in 2014 met succes bij de rechtbank Amsterdam de vorige bestuurders aansprakelijk te stellen, omdat zij de zwakke beveiliging hadden verzwegen voor de kopers. Via hun persoonlijke bv's moesten zij miljoenen euro's terugbetalen. Amerikaanse toestanden in de polder.

Sinds 1 januari 2016 heeft de wetgever bestuurdersaansprakelijkheid expliciet mogelijk gemaakt bij ernstige datalekken. Niet alleen een instructie tot onrechtmatig handelen kan daartoe leiden, ook het laten voortduren ervan of nalaten van preventieve maatregelen te treffen. Momenteel behandelt het parlement een meldplicht beveiligingsincidenten in brede zin, of er nu een datalek is of niet. Een cyberaanval die de energievoorziening, gezondheidszorg

Target en Diginotar tonen hoe cyberaanval grote en kleine onderneming diep in de problemen brengt

of het f... dan m... aandee... nisatie ... verzwakte IT-systemen gebruikt, lopen onderneming en bestuurder een serieus risico. Vooral als het bestuur na interne escalatie pijnlijke feiten verzwijgt of verdraait om onder de radar te blijven.

Niet alleen de media en IT-consultants, zelfs conventionele juridische vaktijdschriften publiceren nu over aansprakelijkheid bij cyberaanvallen. Vorige week verscheen een sterk overzichtsartikel van Eric Tjong Tjin Tai. De Tilburgse hoogleraar privaatrecht is alleen wat te voorzichtig waar hij vermoedt dat de schade na een datalek meevalt. Target en Diginotar tonen hoe een cyberaanval een grote en kleine onderneming diep in de problemen brengt of zelfs de nek omdraait, met miljoenenschade als gevolg.

Daarnaast breidt de nieuwe Nederlandse datawetgeving de handhavingsboetes uit tot maximaal 10% van de binnenlandse jaaromzet. De nieuwe EU-wet, die per mei 2018 de Nederlandse vervangt, maximeert de boete op 4% van de mondiale jaaromzet. Legt een toezichthouder zo'n heftige boete op, dan is er echt iets goed misgegaan en zullen

... de financiële sector kunnen opport... tische stichtingen beperkte individ... dataschade gezamenlijk ophalen b... rechter. Via internet zijn duizenden... ten van een groot bedrijf zo gevond... De naderende beveiligingsnachtm... van het internet der dingen doet no... flinke duit in het zakje. Zie als bestu... der een 'connected' cv-ketel, auto o... visie een jaar na aankoop maar bew... te houden tegen cyberaanvallen.

Beveiliging blijft moeilijk, maar bestuurders kunnen zich niet meer schuilen achter de cybercomplexite... Vooral verdraaien en verzwijgen zal aangepakt worden. Verzekeraars h... hun beurzen dan gesloten. Als cybe... curity vanuit maatschappelijk oogp... nog geen boardroom-issue was, zal... trend richting hoge boetes en bestu... dersaansprakelijk na ernstige cyber... denten daarin het sluitstuk vormen

Axel Arnbak

Axel Arnbak is advocaat bij De Br... Blackstone Westbroek en onderz... aan het Instituut voor Informatier... (UvA). Reacties: **@axelarnbak**

pagina 11, 16-06-2016 © Het Financieele Dagblad

ECONOMIE **33**

INTERVIEW ALEID WOLFSEN

Privacybaas dreigt gemeenten en bedrijven met hoge boetes

Torenhoge boetes wachten bedrijven die slordig omgaan met de privacy van hun klanten. Ook als er geen sprake is van 'grove schuld'.

Ga uw gang als u uw naaktfoto's wilt delen met 20.000 vrienden

Miljoenenboete Facebook is kinderspel bij wat komen gaat

De boete van enkele miljoenen euro's die Facebook boven het hoofd hangt voor het overtreden van de Nederlandse privacywet is kinderspel bij wat de toezichthouder vanaf volgend jaar kan uitdelen. Als de Autoriteit persoonsgegevens (AP) dan, zoals twee weken geleden, oordeelt dat het socialemediabedrijf de gebruikers van het platform op meer punten niet duidelijk informeert over het gebruik van persoonsgegevens, kan ze een maximale boete opleggen van enkele miljarden euro's.

Geen kwantumkorting

'Dit kan heel vervelend worden voor bedrijven', waarschuwt Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens. Nu heeft de privacywaakhond de mogelijkheid Facebook een last onder dwangsom op te leggen, wat neerkomt op een voorwaardelijke boete. Pas als het concern binnen een bepaalde tijd niets tegen de overtredingen doet, wordt de boete onvoorwaardelijk.

Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens. Foto: Wiebe Kiestra

Volgen via mijn nieuws

- Boete
- Compliance
- EU
- Facebook
- Privacy
- Sociale media
- Technologie
- Toezichthouder

Laatste nieuws

21:37
Auteur Franse anti-corruptiewet blijkt zelf geen voorbeeld

21:23
Federal Reserve verhoogt rente ondanks tegenvallende inflatie

21:15
NVWA neemt exclusieve

Beveilig de data passend

grote uitdaging

- Inschakelen van (sub)bewerkers. Onderzoeksrapport: SNAPPET.

de Bibliotheek op school

Home | Toolkit | Opleidingen | Monitor | BOP | Nieuwsberichten | Over | Contact | Films

Waar ben je naar op zoek? Vind

Privacy en de school-bibliotheeksystemen

Gepubliceerd op: 18 april 2017 10:55

Met de gewijzigde bepalingen in de Wet Bescherming Persoonsgegevens (Wbp) is de vraag naar het goed regelen van de privacy toegenomen. Als antwoord hierop zijn twee overeenkomsten toegevoegd aan de set overeenkomsten in de besloten toolkit: een Bewerkersovereenkomst en een Subbewerkersovereenkomst rondom de schoolbibliotheek-systemen. Ook is een toelichting beschikbaar, omdat het goed regelen van de privacy van bibliotheek tot bibliotheek kan verschillen. Tenslotte zijn de Algemene Leveringsvoorwaarden aangepast.

snappet
Connected Learning

Vakblad voor de openbare bibliotheek

bibliotheekblad

Home
Nieuws
Nieuwsoverzicht
Nieuws uitgelicht
Agenda
Nieuwsbrief
Bibliotheekblad
Rubrieken
Dossiers
Beste Bibliotheek
Media

Home > Nieuws > Nieuws uitgelicht > Bericht

OCW wil gegevens afzonderlijke bibliotheken openbaar maken, ondanks bezwaren uit branche

Wim Keizer
19-01-2017

Het ministerie van OCW is van plan op grond van de Wet openbaarheid van bestuur (Wob) te voldoen aan een verzoek om openbaarmaking van gegevens van de afzonderlijke openbare bibliotheken, ondanks bezwaren van de Vereniging van Openbare Bibliotheken (VOB) en 73 openbare bibliotheken.

Dit heeft het ministerie in een mailbericht van 17 januari aan de VOB en de bibliotheken laten weten. Bij het bericht zat een kopie van de brief aan de verzoeker, waarin staat dat OCW het verzoek wil honoreren en om welke redenen de bezwaren van VOB en bibliotheken worden afgewezen. Desgevraagd meldt Aad van Tongeren, senior beleidsadviseur bij OCW, dat de verzoeker een adviesbureau voor de publieke sector is. Dit bureau biedt overheden expertise aan en verzamelt informatie ter onderbouwing van de adviezen.

De gegevens waar het om gaat worden vermeld in bijlage 1 van de Regeling gegevenslevering openbare bibliotheekvoorzieningen: informatie over collectiebezit, uitleningen, leden, uitoefenen kernfuncties, financiën en personeel. Artikel 11 van de Wet stelsel openbare bibliotheekvoorzieningen (Wsob) bepaalt dat de bibliotheken gegevens moeten leveren. Deze mogen niet herleidbaar zijn tot individuele gegevens van gebruikers en personeelsleden. In de brief aan de verzoeker (pdf) meldt OCW dan ook dat er een uitzondering is gemaakt voor dergelijke persoonsgegevens.

- Dataminimalisatie versus openheid van informatiesystemen versus Learning Analytics.

Easier quick wins

- Contracten met ICT leveranciers nalopen
- Privacybeleid formuleren
- Cookiebeleid en privacystatement website
- HR verzuimgegevens & beleidsregels AP
- Netwerkbeveiliging controleren en laten testen
- 2FA toepassen buiten kantooromgeving
- Privacy filters gebruiken en veilige USB-stick
  Datashur)
- PIA uitvoeren HR data
- Datalek beleid formuleren
- Emailbeveiliging op orde maken

Maar blijf verder kijken dan 'the tip'

er bestaat niet zoiets als eenmaal compliant altijd compliant.... zeker niet met het verantwoordingsbeginsel van artikel 5 lid 2 AVG en artikel 24 AVG...

En blijf investeren in ontwikkeling